PLEAD (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:27:02 UTC

PLEAD is a RAT used by the actor BlackTech. FireEye uses the synonyms GOODTIMES for the RAT module and DRAWDOWN for the respective downloader.

2020-12-24 · IronNet ·
China cyber attacks: the current threat landscape
PLEAD TSCookie FlowCloud Lookback PLEAD PlugX Quasar RAT Winnti 2020-12-19 · Cyber And Ramen blog · Mike R
Persistence Pays Off: A Brief Look at BlackTech's 2020
PLEAD TSCookie PLEAD 2020-09-29 · Symantec · Threat Hunter Team
Palmerworm: Espionage Gang Targets the Media, Finance, and Other Sectors
KIVARS PLEAD BlackTech 2019-12-12 · FireEye · Chi-en Shen, Oleg Bondarenko
Cyber Threat Landscape in Japan – Revealing Threat in the Shadow
Cerberus TSCookie Cobalt Strike Dtrack Emotet Formbook IcedID Icefog IRONHALO Loki Password Stealer (PWS) PandaBanker PLEAD POISONPLUG TrickBot BlackTech 2019-11-22 · SANS Cyber Security Summit · Rachel Mullan, Sveva Vittoria Scenarelli
Need for PLEAD: BlackTech Pursuit
BLUETHER PLEAD 2019-10-01 · · Macnica Networks · Macnica Networks
Trends in Cyber Espionage Targeting Japan 1st Half of 2019
PLEAD TSCookie Datper PLEAD 2019-09-18 · JPCERT/CC · Shusei Tomonaga
Malware Used by BlackTech after Network Intrusion
PLEAD 2019-08-01 · Kaspersky Labs · GReAT
APT trends report Q2 2019
ZooPark magecart POWERSTATS Chaperone COMpfun EternalPetya FinFisher RAT HawkEye Keylogger HOPLIGHT Microcin NjRAT Olympic Destroyer PLEAD RokRAT Triton Zebrocy 2019-05-30 · JPCERT/CC · Shusei Tomonaga
Bug in Malware "TSCookie" - Fails to Read Configuration - (Update)
PLEAD 2019-05-14 · ESET Research · Anton Cherepanov
Plead malware distributed via MitM attacks at router level, misusing ASUS WebStorage
PLEAD BlackTech 2019-04-01 · · Macnica Networks · Macnica Networks
Trends in Cyber Espionage Targeting Japan 2nd Half of 2018
Anel Cobalt Strike Datper PLEAD Quasar RAT RedLeaves taidoor Zebrocy 2018-11-12 · JPCERT/CC · Shusei Tomonaga
Bug in Malware "TSCookie" - Fails to Read Configuration
PLEAD 2018-07-09 · ESET Research · Anton Cherepanov
Certificates stolen from Taiwanese tech-companies misused in Plead malware campaign
PLEAD BlackTech 2018-06-08 · JPCERT/CC · Shusei Tomonaga

PLEAD Downloader Used by BlackTech

PLEAD 2018-03-06 · Shusei Tomonaga

Malware “TSCookie”

PLEAD 2018-01-10 · Freebuf · Tencent Computer Manager

Analysis of BlackTech's latest APT attack

PLEAD 2017-06-22 · Trend Micro · CH Lei, Lenart Bermejo, Razor Huang

Following the Trail of BlackTech’s Cyber Espionage Campaigns

PLEAD BlackTech 2017-06-22 · Trend Micro · CH Lei, Lenart Bermejo, Razor Huang

The Trail of BlackTech’s Cyber Espionage Campaigns

bifrose KIVARS PLEAD 2017-06-01 · Trend Micro · CH Lei, Lenart Bermejo, Razor Huang

Following the Trail of BlackTech’s Cyber Espionage Campaigns

PLEAD 2016-04-13 · FireEye · Daniel Regalado, Erye Hernandez, Taha Karim, Varun Jian

Ghosts in the Endpoint

PLEAD 2014-07-02 · Trend Micro · Kervin Alintanahin, Ronnie Giagone

KIVARS With Venom: Targeted Attacks Upgrade with 64-bit “Support”

FakeWord KIVARS PLEAD Poison RAT Zeus

▶ [TLP:WHITE] win_plead_auto (20251219 | Detects win.plead.)
